ABSTRACT

Digital certification method in which a first digital signature dependent upon a first user identity and a first user system in combination, is stored accessibly to a certification server. The first user identity can be distinguished by, for example, a PIN provided by the user. Subsequently, ~~at a second time when the user desires authorization to complete a transaction~~, the user system generates a second signature dependent upon both the current user identity and the current user system in combination. The certifying system then compares the second signature with the first, as stored, ~~in order to determine whether~~ to certify the transaction. The certification can accommodate normal computer system component drift. ~~In an embodiment,~~ An ~~an~~ inquiring system, desiring to confirm the identity of a user, issues a challenge code to the user system. The user system then digests the user's PIN, individual component signatures as they currently exist on the user's system, together with the challenge code to generate the new signature. The new signature is transmitted back to the inquiring system, which transmits it on to the certification server together with the challenge code. The certification server then digests the challenge code with the original signature as previously stored, and compares

the result to the newly provided signature. ~~If they match, then~~ to confirm the user's identity ~~is confirmed,~~ else ~~If not,~~ ~~then~~ drift criteria can be applied if desired.

P.C.